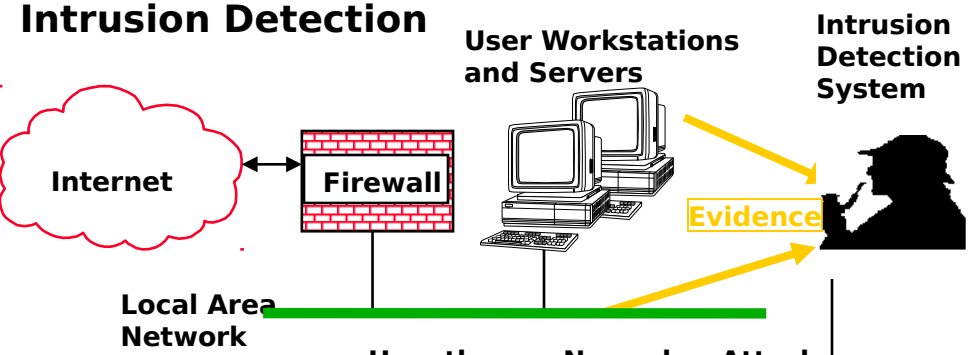
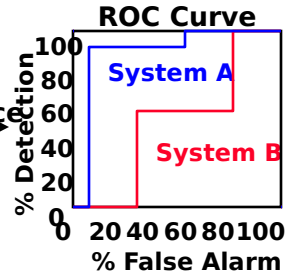
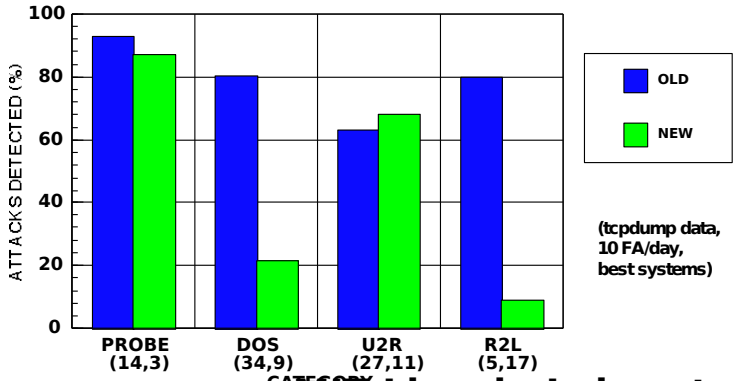
Intrusion Detection Technology Evaluation

Intrusion Detection





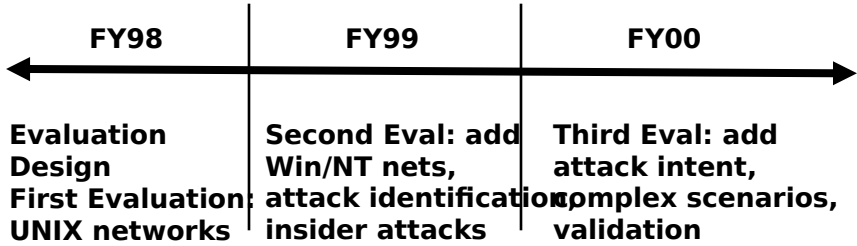
Typical Result



Goals and Impact

- Intrusion detection systems monitor network state looking for unauthorized usage, denial of service, and anomalous behavior
- First careful, objective, repeatable, statistically significant measurement of system performance (probability of detection vs. probability of false alarm) made in FY98… 2nd evaluation in FY99
- Key FY98 eval results: Systems generalize well in some attack categories, but not in others and no single system alone finds even 80% of the attacks at a “reasonable” false alarm rate
- Measurements can be used as references for DoD military and agencies in their selection of intrusion detection products and to guide future government and commercial research

Schedule



MIT Lincoln Laboratory: Richard P. Lippmann and Marc A. Zissman